

REMARKS

The Examiner's allowance of claims 1, 3-21, and indication that claim 24 is drawn to allowable subject matter is noted with appreciation. After careful review of the newly cited reference, the undersigned is of the position that claim 23 is entitled to allowance without further revision, and reconsideration is hereby requested.

In the office action, the Examiner indicated that the drawings filed January 2, 2002 have been accepted. However, in the previous amendment filed June 6, 2005, a spelling error was corrected in Figure 5. Acceptance of this change made June 6, 2004 is requested in the next office action.

Claim 23 has been rejected as being anticipated by U.S. Patent 6,898,708 to Hori et. al. (hereinafter Hori). Applicant respectfully traverses this rejection.

The invention is a system and method for controlling the access to and reproduction of encrypted digital information on a host system. As shown in the preferred embodiment in Fig. 2, after the compression and encryption steps the digital information is conveyed to the host system preferably with one of a plurality of decryption keys (see block 230), however as shown in Fig. 3, block 309, the host system may use alternate means to obtain decryption keys. Referring to Fig. 4, the decryption keys perform two functions. First, each key decrypts the digital information (block 407). Second, each key controls host system software, for example the media player application, to effect a different level and/or type of reproduction quality degradation on the media player (block 410). The level and type of reproduction quality degradation may be controlled by a time condition or a use condition, or alternatively, reproduction may be limited to only a portion of the digital information sought by the user. For example, quality may be degraded to a point where there is slight degradation (e.g., where coloration of the images are altered), or substantial or complete degradation may be effected (e.g., a scrambling effect or even a dark screen). To control reproduction quality in this manner, the media player application preferably accesses a table of information which correlates each of the types of decryption keys with a certain reproduction

quality. Ultimately, the user can purchase or otherwise obtain the decryption key referenced in block 310 of Fig. 3, which allows for continued viewing of the digital information without degradation.

One object of the present invention is to initially restrict access to only a portion of the digital information when reproduced on the host system (page 3, lines 10-11). Claim 23 is focused on one particular embodiment of the invention where a first decryption key allows the application program reproducing the digital information to reproduce only a portion of the digital information. Claim 24 is dependent on claim 23, and provides for a second decryption key at the host which allows for reproducing all of the digital information. This allows for a user to view a portion of the digital information before making a decision to purchase or otherwise obtain the second decryption key to reproduce the digital information in its entirety.

On page 3 of the Examiner's Response, the Examiner stated that Hori teaches the use of a first decryption key stored on a host system to control an application program, also stored on a host system, to reproduce only a portion of the digital information. This is an incorrect reading of Hori.

Hori teaches a data distribution system using a plurality of keys to encrypt and decrypt data and retain session logs (see Fig. 2). For example, each content reproducing circuit (i.e., cellular phone) and memory card have associated keys (col. 8, lines 4-13), and unique session keys are generated in response to every distribution session, transfer session, and reproduction session (col. 9, lines 20-42). The system requires the generation of certain key combinations in certain orders before allowing the reproduction of data (see, e.g., Figs. 6-13). Once the sequence of key combinations is complete, the requested data is reproduced in the reproducing circuit in its entirety (Fig. 7, S236). However, Hori does not teach the use of any number of decryption keys to reproduce only a portion of stored data. Further, Hori does not teach the use of an additional decryption key to allow the reproduction of stored data in its entirety. The passage cited by the Examiner, col. 11, lines 8-25, deals with various components of the cellular phone and memory card as taught by Hori. These components include a decryption key holding

portion (Fig. 4, 1502), a decryption processing portion (1504, 1510), a session key generation portion (1508), and an encryption processing portion (1506). None of these portions involve the use of a decryption key to allow reproduction of only a portion of stored data (col. 11, lines 8-25).

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1, 3-24 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 09-0457.

Respectfully submitted,



Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 30743